Przegląd Strategiczny 2014, nr 7

Jędrzej SKRZYPCZAK
Uniwersytet im. Adama Mickiewicza w Poznaniu

DOI 10.14746/ps.2014.1.10

POLITYKA OCHRONY CYBERPRZESTRZENI RP

Masowe wykorzystywanie urządzeń i technologii teleinformatycznych (ang. *information and communication technologies* – ICT) w różnych obszarach i sferach życia publicznego i społecznego powoduje, iż konieczne staje się zapewnienie należytej ochrony infrastruktury informatycznej. W ramach procesu cyfryzacji państwa, technologie takie wykorzystywane są przez instytucje publiczne (instytucje administracji rządowej i samorządowej, władzy ustawodawczej, wykonawczej i sądowniczej), służby wyspecjalizowane (np. policja, pogotowie, straż pożarna) media, instytucje bankowo-finansowe w ramach oferowanych usług, transport (lotniczy, kolejowy), sieci energetyczno-wodociągowe (Suchorzewska, 2010: 318–338). Większość tych obszarów miesi się w ramach tzw. infrastruktury krytycznej, rozumianej jako sieci powiązanych ze sobą systemów zapewniających instytucjom państwowym, gospodarczym i społecznym możliwość realizacji podstawowych zadań, takich jak utrzymanie bezpieczeństwa i porządku publicznego oraz dostarczanie podstawowych usług społecznych (Dawidziak, Łącki, Stolarski, 2009: 55–56).

Przestrzeń wirtualna, cyfrowa zaczyna być traktowana jak terytorium danego państwa. Pojawiają się chociażby takie pojęcia jak cyberprzestrzeń państwa. W tym kontekście warto zwrócić uwagę na dokument zatytułowany Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej, przyjęty w 2013 przez *Ministerstwo Administracji i Cyfryzacji* i *Agencję Bezpieczeństwa Wewnętrznego* (*Polityka*, 2013). Zdefiniowano tu pojęcie „cyberprzestrzeni" i „cyberprzestrzeni Rzeczpospolitej Polskiej". Ten pierwszy definiowany jest jako „przestrzeń przetwarzania i wymiany informacji, tworzona przez systemy teleinformacyjne, określone w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne (*Ustawa*, 2005; *Polityka*, 2013). Z kolei ten drugi pojmowany jest jako „cyberprzestrzeń w obrębie terytorium państwa polskiego i poza jego terytorium w miejscach, gdzie funkcjonują przedstawiciele RP tj. placówki dyplomatyczne, kontyngenty wojskowe" (*Polityka*, 2013). Zwraca uwagę powiązanie cyberprzestrzeni z terytorium państwa polskiego w ujęciu fizycznym i prawnym. Warto w tym miejscu przypomnieć, że w ustawie z 12 października 1990 r. o ochronie granicy państwowej (*Ustawa*, 1990) za terytorium Rzeczypospolitej Polskiej uznaje się „obszar objęty granicami państwowymi, oddzielającymi terytorium Rzeczypospolitej Polskiej od terytorium innych państw i morza pełnego, wody wewnętrzne i pas morskich wód terytorialnych oraz przestrzeń powietrzną nad tym obszarem i wnętrze ziemi pod nim" (*Kodeks*, 2004).

Jak widać w przypadku cytowanego dokumentu – bodaj po raz pierwszy – próbowano zdefiniować obszar kognicji polskiego porządku prawnego w obszarze wirtualnej rzeczywistości cyfrowej jak również obszar wpływów. Taki zabieg jest o tyle ryzykowny, iż w istocie przestrzeń wirtualna jest przecież niematerialna i aterytorialna,

niepodlegająca władztwu żadnego państwa. Pojawiają się także terminy obrazujące zjawiska ze świata realnego zachodzące również w świecie wirtualnym, takie jak np.: atak, działalność przestępcza, terroryzm w cyberprzestrzeni. I tak, w myśl postanowień tego dokumentu, „cyberatak" to celowe zakłócenie prawidłowego funkcjonowania cyberprzestrzeni, a „cyberprzestępstwo" to czyn zabroniony popełniony w obszarze cyberprzestrzeni, natomiast cyberterroryzm to przestępstwo o charakterze terrorystycznym popełnione w cyberprzestrzeni, a „incydent związany z bezpieczeństwem informacji" to pojedyncze zdarzenie lub seria niepożądanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji" (*Polityka*, 2013).

Podnosi się w doktrynie, że zagrożeń dla tego obszaru można upatrywać paradoksalnie w samej istocie i architekturze tej sieci informatycznej, podnosząc takie elementy jak: masowa skala punktów wejścia, ilość powiązanych ze sobą elementów struktury społecznej, możliwość uzyskania anonimowości, transgraniczny i światowy charakter przekazu, aterytorialność i niematerialność cyberprzestrzeni. Trzeba bowiem podkreślić, że Internet składa się z wielu niezależnie od siebie działających ogniw i tzw. hub-ów, co oznacza, iż uszkodzenie lub zniszczenie jednego lub nawet wielu elementów nie powinno zakłócać funkcjonowania całości systemu (Madej, 2009: 23–25). Właśnie to założenie legło u podstawy budowy Internetu, jak i jego protoplasty, czyli *ARPANET-u*, co oczywiście wynikało z chęci zapewnienia bezpieczeństwa poszczególnym, rozproszonym węzłom łączności w przypadku ataku jądrowego. Podnosi się jednak dziś, że nie ma pewności, czy zniszczenie poszczególnych elementów, nawet peryferyjnych, nie spowoduje zakłóceń stabilności całego systemu. Ponadto należy zauważyć, iż zdecydowana większość elementów sieci teleinformatycznych nie jest własnością państw, tylko sektora prywatnego, co powoduje, że wpływ instytucji publicznych w tym zakresie jest z natury rzeczy ograniczony. Co może być istotne, podmioty zarządzające internetem, takie jak ICANN (the *Internet Corporation for Assigned Numbers and Names*), IANA (*Internet Assigned Numbers Authority*), mają siedziby w USA i podlegają prawu amerykańskiemu (*Communication*, 2000). Stąd, zwłaszcza po aferze ujawnionej przez Edwarda Snowndena, związanej z bezprawną ingerencją przez *National Security Agency* (NSA) w sferę tajemnicy korespondencji elektronicznej i podsłuchiwanie rozmów telefonicznych przywódców państw, pojawiły się pomysły na stworzenie odrębnej, europejskiej sieci telekomunikacyjnej (*Europejski*, 2014). Dla oceny słabych stron tego systemu, nie bez znaczenia jest także, że mamy do czynienia z dominacją określonych, jednolitych rozwiązań i systemów informatycznych w skali wręcz światowej, co powoduje łatwość przenoszenia „infekcji". Poważnych zagrożeń upatrywać można w takich zjawiskach jak: rozpowszechnianie szkodliwych narzędzi informatycznych (programy hakerskie, wirusy), niszczenie lub uszkadzanie infrastruktury teleinformatycznej, co w konsekwencji prowadzić może do zniszczeń w świecie realnym, a nawet zagrożeń dla zdrowia i życia obywateli, modyfikacji przechowywanych w standardach cyfrowych informacji, a wreszcie działań dezinformacyjnych (Madej, 2009: 23–25). Obecnie nie tylko sektor medialny staje się wytwórcą komunikatów i treści, ale właściwie każdy członek społeczności. Dzięki powstaniu tzw. mediów społecznościowych obecnych na różnych platformach komunikacji i powszechnej dostępności miniaturowych urządzeń (np. smartfonów wyposażonych w ka-

mery nawet w standardzie HD), każdy może stać się twórcą określonego komunikatu i przekazu audiowizualnego. Stąd też nawet najmniejsze zdarzenie krytyczne, może zostać wykreowane na wydarzenie przykuwające uwagę milionów obywateli. To z kolei może prowadzić do łatwego manipulowania zachowaniem danych grup. Stwarza to oczywiście doskonałe możliwości dla osiągnięcia efektu tzw. *force equalizer*, a więc możliwość równoważenia potencjału instytucji państwowych przez małe grupy, a nawet jednostki. Stąd też uznać należy, że sieć staje się idealnym środowiskiem dla różnorodnych tzw. zagrożeń asymetrycznych (ibidem: 31). Dlatego wskazuje się na pojawienie się takiego zjawiska jak tzw. cyberterroryzm, czyli „politycznie umotywowana, przemyślana działalność grup narodowych lub innych wrogich sił wymierzona przeciw informacji, systemom komputerowym, programom i danym, która powoduje straty cywilne" (Krasavin, 2002). Według innej definicji to „jakiekolwiek użycie informacyjnej technologii i wiedzy przez agentów lub grupy terrorystyczne" (Bógdał-Brzezińska, Gawrycki, 2003: 65–66) albo „działania blokujące, mieszczące lub zniekształcające w stosunku do informacji przetwarzanej, przechowywanej i przekazywanej w systemach teleinformatycznych oraz niszczące (obezwładniające) te systemy" (ibidem). Przyjmuje się, że pierwszym zamachem cyberterrorystycznym był atak z 1998 r. dokonany przez partyzantkę *Tamilskich Tygrysów*, przez wysyłanie masowo listów na skrzynki mailowe ambasady Sri Lanki (Suchorzewska, 2010: 57). Innym przypadkiem był incydent z Australii, polegający na tym, że informatyk nieprzyjęty do pracy, w akcie zemsty dokonał ataku na system komputerowy sterujący przepływem ścieków, powodując znaczne zniszczenia środowiska naturalnego. Jeszcze inny przykład to użycie wirusa *Slammer* do zainfekowania systemu informatycznego elektrowni jądrowej w Oak Harbor w Ohio i wyłączenia systemów monitorujących bezpieczeństwo tej placówki. Jednocześnie trzeba zaznaczyć, że nie można cyberterroryzmu utożsamiać z tzw. cyberprzestępczością i działaniami hakerskimi. Zauważa się bowiem, że: „terroryzm jest po porostu jednym z typów międzynarodowej działalności kryminalnej dokonywanej przez Internet". Cyberterrozym próbuje się zwalczać podobnymi środkami jak cyberprzestępstwa, ale są to dwa różne zjawiska, do których powinno się stosować inne instrumenty (Sheehan, 2000; Bógdał-Brzezińska, Gawrycki, 2003: 66–68). Wyjaśnić należy tu także pojęcie tzw. walki informacyjnej, czyli „akcji mających na celu osiągnięcie wyższości informacyjnej poprzez oddziaływanie na informację przeciwnika, jego system informacyjny, proces przepływu informacji i sieci komputerowe oraz obronę własnych informacji, systemów informacyjnych, procesów przepływu informacji i sieci komputerowych" (Ciborowski, 1997: 35–37; Bógdał-Brzezińska, Gawrycki, 2003: 66–68). Przy czym wskazuje się na wiele form prowadzenia takiej walki, a mianowicie:

– *command-and-control warfare* – której celem jest uzyskanie przewagi w dowodzeniu;
– *intelligence-based warfare* – bazującej na wiedzy rozpoznawczej;
– *electronic warfare* – nakierowanej na techniki radioelektroniczne i kryptograficzne;
– *psychological warfare* – walka psychologiczna;
– *hacker warfare* – atak na systemy informacyjne;
– *economic information warfare* – blokowanie informacji w celu osiągnięcia przewagi ekonomicznej;

– *cyberwarfare* – wojna w rzeczywistości wirtualnej (Libicki, 1995: 7; Bógdał-Brzezińska, Gawrycki, 2003: 68).

Jak się podkreśla, jednym z podstawowych kryteriów rozróżniających walkę (wojnę) informacyjną od cyberterrorzymu jest wskazanie podmiotu odpowiedzialnego za takie działania. I tak, jeżeli inicjatorem takich akcji jest określone państwo, a działanie ma charakter zorganizowany i niekierowane jest na uzyskanie informacyjnej dominacji, to mamy do czynienia z walką informacyjną, jeżeli zaś aktywność taką inicjuje podmiot niepaństwowy i ma ona charakter zwykle spontaniczny i chodzi o uderzenie w słaby punkt wroga, to można mówić o cyberterroryzmie (Libicki, 1995: 7; Bógdał-Brzezińska, Gawrycki, 2003: 68). Jednak zdaniem innych autorów, takie pojęcia jak: „cyberwar, infowar, walka informacyjna, netwar, cyberpunks, informacyjni wojownicy, informacyjna dominacja, obrona w cyberprzestrzeni […] informacyjny chaos […], to tylko neologizmy dotyczące tego samego, ale bardzo szerokiego pojęcia – wojny ery informacyjnej (information – age warefare)" (Sanz, 1998; Bógdał-Brzezińska, Gawrycki, 2003: 71). Niektórzy jako przykład takiej działalności, wskazują doświadczenia Estonii, która w związku z dynamicznym rozwojem usieciowania, szerokim wdrożeniem e-administracji, zasłużyła, aby nazywać to państwo jako „E-stonia". Otóż na przełomie kwietnia i maja 2007 r. dokonano ataku na strony internetowe najważniejszych instytucji publicznych, takich jak kancelarii prezydenta, rządu, ministerstw, partii politycznych, agencji informacyjnych oraz największych banków. Jako winnego tych działań wskazywano Rosję, choć nigdy władze Federacji Rosyjskiej nie przyznały się do winy. Co ciekawe, w 2008 r. podobna sytuacja powtórzyła się w Gruzji, a w 2014 r. na Ukrainie z użyciem wirusa *Snake*. Ponadto w tej grupie podobnych incydentów, wskazuje się także konflikt w Kosowie (Suchorzewska, 2010: 66–68).

Wyjaśnić w tym miejscu wypada także takie zjawiska jak aktywizm i haktywizm. Ten pierwszy termin oznacza „niedestrukcyjne wykorzystanie Internetu dla wspierania prowadzonych działań […]. Aktywiści wykorzystują Internet w pięciu ściśle określonych, aczkolwiek występujących wspólnie celach: zbierania informacji, publikacji i prezentacji własnych poglądów, komunikacji (porozumiewanie się z innymi), koordynacji prowadzonych działań oraz lobowania na rzecz wybranych rozwiązań […]. Wyróżnić można jego bierną i czynną formę. Bierność to zwykle poszukiwanie informacji oraz przyłączanie się do istniejących grup dyskusyjnych, forma czynna aktywizmu to natomiast samodzielne prowadzenie działań informacyjnych, dzielenie się własnymi poglądami, publikowanie tekstów, zakładanie witryn, przygotowanie apeli oraz rozsyłanie informacji" (ibidem: 64). Jako przykład wskazuje się aktywność grupy dyskusyjnej *Uncrypto*, zaangażowanej w sprawy kryptografii i brytyjskich regulacjach prawnych tego zagadnienia. Bardzo często przybiera postać masowego wysyłania maili w celu poparcia jakiejś inicjatywy lub przyłączenia się do protestów (np. Serbowie masowo wysyłali maile do zachodnich instytucji publicznych w celu przekonania do zaniechania bombardowań w czasie wojny w Kosowie). Inny przykład dotyczy działań zmierzających do unikania cenzury w takich państwach jak np. ChRL czy Kuba.

Z kolei haktywizm to termin powstały w wyniku połączenia aktywizmu i hakerstwa, polegający na masowym atakowaniu celów internetowych. Chodzi o tzw. rozproszony atak blokujący serwis (ang. *Distributed Denial of Service*), zmierzający do blokowania określonych witryn internetowych (w wyniku ilości przesyłanych informa-

cji dochodzi do ich przeciążenia i wyłączenia), w celu poparcia określonej idei lub inicjatywy (Dawidziuk, Łącki, Stolarski, 2009: 51–52). Zjawisko haktywizmu powstało w połowie lat 90. XX w. w związku z rozwojem ruchu anty- i alterglobalistycznego. Jest to nawiązanie do tzw. nieposłuszeństwa obywatelskiego, które manifestowało się w zachowaniu polegającym na wtargnięciu do określonego obiektu i jego blokadzie. Funkcjonują w związku z tym takie pojęcia jak *electronic civil disobedience*. Istotą jest nawiązanie do idei anarchizmu i libertanizmu informacyjnego. Jako przykład można wskazać działalność takich grup jak *Netstrike*, *Electronic Disturbance Theater*, *Electrohippies*. Tego rodzaju akcje polegały bądź na wzywaniu do masowego łączenia się o ustalonej godzinie przez internautów z określonym adresem sieciowym, bądź na rozpropagowaniu oprogramowania, które pozwala na automatyczne osiągnięcie powyższego celu. Tak stało się w 1999 r. kiedy *Electrohipisi* dokonali ataku na konferencję WHO w Seattle. Inny rodzaj działalności tego nurtu to zapewnienie bezwzględnego dostępu do szeroko rozumianych zasobów informacyjnych. W związku z tym udostępnianie oprogramowania, które miało uniemożliwić identyfikację internauty. I tak np. w 2006 r. udostępniono anonimową przeglądarkę internetową, która zapewniała m.in. dzięki częstej zmiany IP, anonimowość w internecie. Jeszcze inny sposób to stosowanie sieci *Tor*, czyli rozproszonej sieci komputerowej, która tworzy tzw. chmurę połączonych komputerów (ang. *cloud computing*). W rezultacie powstaje „wirtualny obwód", czyli szereg komputerów, połączonych krótkotrwale przez zakodowane połączenia, zrywanych i ponownie łączących się w krótkich okresach czasu, co może uniemożliwić identyfikację konkretnego użytkownika. Inną płaszczyzną, do której wykorzystuje się opisywane zjawisko, jest ruch na rzecz wolnego lub otwartego oprogramowania. Jako przykład wskazać można akcję tzw. *Anonymous* m.in. w Polsce i innych państwach w związku z próbą podpisania *ACTA* (ang. *Anti-Counterfeiting Trade Agreement*). Inne oprogramowanie tego typu to *Camera Shy*, *Scatterchat* (Jordan, 2011: 89–97).

W kontekście powyższych uwag warto poddać analizie założenia polityki państwa w zakresie zapewnienia bezpieczeństwa cyberprzestrzeni. Warto zwrócić uwagę na wspomniany już powyżej, a przyjęty 25 czerwca 2013 r. przez *Ministerstwo Administracji i Cyfryzacji* oraz Agencję Bezpieczeństwa Wewnętrznego, dokument zatytułowany *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej*. Należy podkreślić, że dokument – choć w znacznej mierze dotyczy zapewnienia bezpieczeństwa teleinformatycznego systemom teleinformatycznym eksploatowanym przez administrację rządową, organy władzy ustawodawczej, władzę sądowniczą, organy samorządu terytorialnego oraz systemom strategicznym – odnosi się także w tej sferze do przedsiębiorców i osób fizycznych. Pojawiła się tu wyraźna deklaracja, iż Rząd RP zobowiązuje się brać czynny udział w zapewnieniu bezpieczeństwa zasobom informacyjnym Państwa, ale także jego obywateli. Jednocześnie zaznaczono, że dokument nie obejmuje tego obszaru odnoszącego się do niejawnych systemów teleinformatycznych. Ten sektor posiada bowiem własne regulacje prawne, a wśród nich w szczególności *Ustawę o ochronie informacji niejawnych* z 5 sierpnia 2010 r. (*Ustawa*, 2010), a także stosowne mechanizmy ochronne oraz struktury organizacyjne dedykowane do ochrony informacji niejawnych wytwarzanych, przetwarzanych oraz przechowywanych w wydzielonych systemach teleinformatycznych. W obszarze militarnym rolę podmiotu realizującego zadania w zakresie zapewnienia bezpieczeństwa teleinformatycznego, powierzono *Re-*

sortowemu Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych.

Jak podkreśla się w cytowanym dokumencie, celem strategicznym polityki ochrony cyberprzestrzeni, jest osiągnięcie akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni Państwa (*Polityka*, 2013). Pojawia się zatem kategoria akceptowalnego poziomu bezpieczeństwa, co jest – jak się wydaje wyrazem realizmu twórców tych założeń. Osiągnięcie zakładanego celu strategicznego ma być, w myśl postanowień tego aktu, realizowane poprzez stworzenie ram organizacyjno-prawnych oraz systemu skutecznej koordynacji i wymiany informacji pomiędzy użytkownikami CRP. Jednocześnie podkreślono, że w tym obszarze konieczne jest zwiększenie poziomu bezpieczeństwa infrastruktury teleinformatycznej Państwa, zdolności do zapobiegania i zwalczania zagrożeń ze strony cyberprzestrzeni, zmniejszenie skutków incydentów godzących w bezpieczeństwo teleinformatyczne, określenie kompetencji podmiotów odpowiedzialnych za bezpieczeństwo cyberprzestrzeni, stworzenie i realizacja spójnego dla wszystkich podmiotów administracji rządowej systemu zarządzania bezpieczeństwem cyberprzestrzeni oraz ustanowienie wytycznych w tym zakresie dla podmiotów niepublicznych, a wreszcie stworzenie trwałego systemu koordynacji i wymiany informacji pomiędzy podmiotami odpowiedzialnymi za bezpieczeństwo cyberprzestrzeni i użytkownikami cyberprzestrzeni, a nadto zwiększenie świadomości użytkowników cyberprzestrzeni w zakresie metod i środków bezpieczeństwa. Zgodnie z założeniami omawianej strategii, powyższe cele realizowane są poprzez: system koordynacji przeciwdziałania i reagowania na zagrożenia i ataki na cyberprzestrzeń, powszechne wdrożenie wśród jednostek administracji rządowej oraz podmiotów niepublicznych, mechanizmów służących zapobieganiu i wczesnemu wykrywaniu zagrożeń oraz właściwego postępowania w przypadku incydentów, a także edukację szerokich rzesz społeczeństwa w tym obszarze (*Polityka*, 2013).

Komentowany dokument stoi na stanowisku, iż podmiotem koordynującym realizację powyższych celów jest *Minister Administracji i Cyfryzacji*, natomiast w zakresie realizacji zadań związanych z bezpieczeństwem *Rządowy Zespół reagowania na Incydenty Komputerowe CERT.GOV.Pl*, jako główny podmiot w obszarze cywilnym. Jego podstawowym zadaniem jest zapewnienie i rozwijanie zdolności jednostek organizacyjnych administracji publicznej RP do ochrony przed cyberzagrożeniami, w szczególności ataków ukierunkowanych na infrastrukturę obejmującą systemy i sieci teleinformatyczne, których zniszczenie lub zakłócenie mogłoby stanowić zagrożenie dla życia i zdrowia ludzi, dziedzictwa narodowego, środowiska naturalnego w znacznych rozmiarach albo spowodować poważne straty materialne lub zakłócić funkcjonowanie państwa. Jak już wyżej wspomniano, w obszarze militarnym rolę taką powierzono *Resortowemu Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych*. Można zatem przyjąć, że zgodnie z postanowieniami dokumentu ustanowiono trzypoziomowy *Krajowy System Reagowania na Incydenty Komputerowe* w CRP: poziom I – poziom koordynacji *MAiC*, poziom II – reagowania na incydenty komputerowe:

– *Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.Pl CERT* (ang. *Computer Emergency Response Team*; ang. *Computer Security Incydent Response Team* CSIRT), czyli zespół powołany do reakcji na zdarzenia naruszające bezpieczeństwo w Internecie, będący jednoczenie głównym narodowym zespołem odpowiedzialnym za koordynowanie procesu reagowania na incydenty komputerowe w CRP; oraz

– *Resortowe Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych*, realizujące zadania w sferze militarnej, poziom III – poziom realizacji – administratorzy poszczególnych systemów informatycznych.

Można oczekiwać, że zbudowany w taki sposób system reagowania, zapewnia wymianę informacji pomiędzy zespołami administracji publicznej oraz zespołami *CERT* (*CERT Polska*, *TP CERT*, *PIONIERCERT*), *CSIRT*, *ABUSE*, przedsiębiorcami telekomunikacyjnymi i usługodawcami świadczącymi usługi drogą elektroniczną, zgodnie z obowiązującymi przepisami prawa, a w szczególności zgodnie z ustawą o ochronie danych osobowych oraz ustawą o ochronie informacji niejawnych (*Polityka*, 2013).

Warto zwrócić uwagę na jeszcze jedną kwestię, a mianowicie jednym z zadań realizowanych w ramach komentowanej Polityki, jest szacowanie ryzyka ewentualnego zagrożenia bezpieczeństwa cyberprzestrzeni, w celu obniżenia takiego zagrożenia do akceptowalnego poziomu. Zobowiązano wszystkie jednostki administracji rządowej, do przedstawiania *MAiC* co roku do 31 stycznia, sprawozdania podsumowującego wyniki szacowanego ryzyka. Co ważne, naruszenie zasad określonych w Polityce, może być przyczyną wykluczenia się podmiotu ze społeczności informacyjnej i powstania utrudnień w dostępie do informacji publicznej. Nie ma natomiast wskazanych podstaw prawnych, ani bliższych wytycznych, jak miałoby się taki skutek osiągnąć. Jest to oczywiste nawiązanie do podobnych rozwiązań prawnych znanych z takich krajów jak np. Francja.

Warto także odnotować inne elementy składające się na infrastrukturę bezpieczeństwa informatycznego w Polsce, rozumianą jako zespół przedsięwzięć o charakterze organizacyjno-prawnych, mających na celu zapewnienie niezakłóconego funkcjonowania cyberprzestrzeni (ibidem). I tak w *Białej Księdze Bezpieczeństwa Narodowego RP* (*Biała*, 2013: 65–67) doceniono ten obszar, podkreślając, iż jest to obecnie jedno z podstawowych zadań strategicznych państwa. W zaprezentowanej diagnozie stwierdza się, że procedury i regulacje dotyczące wymiany informacji o sposobach i taktyce działania przestępców nie są doskonałe. Wskazano, że jeżeli chodzi o budowanie „infrastruktury prawnej" cyberbezpieczeństwa, uczyniono już sporo. W tym katalogu wymienia się: utworzenie w 2011 r. *Ministerstwa Administracji i Cyfryzacji*, dysponującego pełnią kompetencji w dziedzinie informatyzacji i łączności, powołanie specjalistycznej komórki odpowiedzialnej za bezpieczeństwo teleinformatyczne, wprowadzenie zmian w regulacjach prawnych, które pozwalają zastosować odpowiednie mechanizmy prawne w sytuacji niebezpiecznych zjawisk w tej przestrzeni (stany nadzwyczajne). Nie można także pominąć innych dokumentów wpisujących się w politykę ochrony cyberprzestrzeni RP. 9 marca 2009 r. został przyjęty przez *Komitet Stały Rady Ministrów* dokument zatytułowany *Rządowy program ochrony cyberprzestrzeni RP na lata 2009–2011– założenia* (*Rządowy*, 2009). Ponadto przyjmowano okresowe raporty o stanie bezpieczeństwa cyberprzestrzeni, publikowane przez Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL. Trzeba także dostrzec decyzję Przewodniczącego *Komitetu Rady Ministrów do spraw Cyfryzacji* nr 1/2012 z 24 stycznia 2012 r. w przedmiocie powołania zespołu zadaniowego do spraw ochrony portali rządowych.

Ponadto dokonano wielu zmian w powszechnie obowiązujących przepisach prawnych, dostosowując je do ewentualnych zagrożeń w cyberprzestrzeni. Dotyczy to w szczególności regulacji tzw. stanów nadzwyczajnych. We wszystkich aktach normatywnych dotyczących stanów nadzwyczajnych, wpisano niepożądane zdarzenia w cyberprze-

strzeni jako powód wprowadzania jednego ze stanów nadzwyczajnych. I tak w *Ustawie o stanie klęski żywiołowej* z 18 kwietnia 2002 r. (*Ustawa*, 2002b) stanowi się, że stan taki może być wprowadzony dla zapobieżenia m.in. awariom technicznym noszącym znamiona klęski żywiołowej oraz w celu ich usunięcia, przy czym w art. 3 tego aktu normatywnego, jako jedną z przyczyn, które mogą wywołać katastrofę naturalną lub awarię techniczną, wymienia się właśnie zdarzenia w cyberprzestrzeni. Podobnie w *Ustawie o stanie wyjątkowym* z 21 czerwca 2002 r. (*Ustawa*, 2002c) przewidziano, iż w sytuacji szczególnego zagrożenia konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego, w tym m.in. spowodowanego działaniami w cyberprzestrzeni, które nie może być usunięte poprzez użycie zwykłych środków konstytucyjnych, Rada Ministrów może podjąć uchwałę o skierowaniu do Prezydenta Rzeczypospolitej Polskiej wniosku o wprowadzenie stanu wyjątkowego. Wreszcie w *Ustawie o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej* z 29 sierpnia 2002 r. (*Ustawa*, 2002d) stanowi się, że w razie zewnętrznego zagrożenia państwa, w tym spowodowanego działaniami m.in. w cyberprzestrzeni, Prezydent Rzeczypospolitej Polskiej może, na wniosek Rady Ministrów, wprowadzić stan wojenny na części albo na całym terytorium państwa.

Warto także przypomnieć inne akty normatywne, które wpisują się w opisywaną tu politykę ochrony cyberprzestrzeni. I tak w *Rozporządzeniu Prezesa Rady Ministrów w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego* z 20 lipca 2011 r. poddano regulacji: podstawowe wymagania bezpieczeństwa teleinformatycznego, jakim powinny odpowiadać systemy teleinformatyczne oraz niezbędne dane, jakie powinna zawierać dokumentacja bezpieczeństwa systemów teleinformatycznych oraz sposób jej opracowywania. Odpowiednie struktury organizacyjne wyodrębniono w służbach specjalnych. Wspomnieć tu należy o *Zarządzeniu nr 73 Prezesa Rady Ministrów w sprawie nadania statutu Agencji Bezpieczeństwa Wewnętrznego* z 26 czerwca 2002 r., przewidujące wyodrębnienie w ramach tej służby *Departamentu Bezpieczeństwa Teleinformatycznego* (Departament I). Z kolei w *Zarządzeniu Ministra Obrony Narodowej w sprawie nadania statutu Służbie Kontrwywiadu Wojskowego (SKW)* z 20 października 2006 r., w § 3 ust. 1 stanowi się, że w strukturze tej służby funkcjonuje jednostka organizacyjna odpowiedzialna za poruszaną tu problematykę, a mianowicie *Biuro Bezpieczeństwa Teleinformatycznego*.

Ponadto w Kodeksie karnym (*Ustawa*, 1997) stypizowano wiele czynów zabronionych, których sposób popełnienia wiąże się z wykorzystaniem cyberprzestrzeni (Adamski, 2001: 17). I tak, przewidziano tu odpowiedzialność karną za takie czyny jak: tzw. *hacking*, czyli uzyskanie bez uprawnień dostępu do informacji nieprzeznaczonej dla danej osoby, m.in. poprzez podłączenie się do sieci telekomunikacyjnej lub uzyskanie nieuprawnionego dostępu do systemu informatycznego (Fischer, 2000: 63–66). Jak wskazuje się w doktrynie, przedmiotem ochrony przestępstwa opisanego w art. 267 k.k., jest zabezpieczenie informacji będących w dyspozycji określonej osoby przed osobami nieuprawnionymi (Adamski, 2000: 45; Kuźnicka-Michalska, 2010: 691; Hałas, 2012: 1143; Siwicki, 2013: 109; Wróbel, 2013: 1498–1505; Adamski, 1998). Odrębnym przestępstwem stypizowanym w Kodeksie karnym (art. 268), jest naruszenie integralności komputerowego spisu informacji, polegające na niezgodnym z pra-

wem niszczeniu, uszkadzaniu, usuwaniu lub zmienianiu zapisu istotnej informacji (Adamski, 2000: 64; Siwicki, 2013: 142–146, Wróbel, 2013: 1512–1515). Zgodnie z kolei z treścią z art. 268a k.k. czynem zabronionym zagrożonym karą, jest także zachowanie polegające na nieuprawnionym niszczeniu, uszkadzaniu, usuwaniu, zmienianiu lub utrudnianiu dostępu do danych informatycznych albo zakłócaniu lub uniemożliwianiu automatycznego przetwarzania, gromadzenia lub przekazywania takich danych (Siwicki, 2013: 147–150; Wróbel, 2013: 1518). W art. 269 k.k. przewidziano przestępstwo tzw. sabotażu informacyjnego, polegające na niszczeniu, uszkadzaniu, usuwaniu lub zmienianiu danych informatycznych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, samorządowej (Adamski, 2000: 76; Siwicki, 2013: 157; Wróbel, 2013: 1522–1522). Z kolei zgodnie z art. 269a. k.k. odpowiedzialności karnej podlegać będzie ten kto – nie będąc do tego uprawnionym – przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu komputerowego lub sieci teleinformatycznej (Siwicki, 2013: 159; Wróbel, 2013: 1526–1527). Wreszcie, w myśl z art. 269b k.k., każdy kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia wyżej określonych przestępstw, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej podlega odpowiedzialności karnej (Wróbel, 2013: 1528–1531).

Choć może to niepokoić, to nie ma wątpliwości, iż (zważywszy m.in. na specyfikę Internetu) zapewnienie 100% stanu bezpieczeństwa teleinformatycznego, jest właściwie niemożliwe. Można mówić jedynie o osiągnięciu pewnego, akceptowalnego jego poziomu. Do osiągnięcia tego celu, mają służyć priorytety polityki ochrony cyberprzestrzeni RP, a wśród nich w szczególności określenie kompetencji podmiotów odpowiedzialnych za bezpieczeństwo cyberprzestrzeni, stworzenie i realizacja spójnego dla wszystkich podmiotów administracji rządowej systemu zarządzania bezpieczeństwem cyberprzestrzeni oraz ustanowienie wytycznych w tym zakresie dla podmiotów niepublicznych, stworzenie trwałego systemu koordynacji i wymiany informacji pomiędzy podmiotami odpowiedzialnymi za bezpieczeństwo cyberprzestrzeni i użytkownikami cyberprzestrzeni, zwiększenie świadomości użytkowników cyberprzestrzeni w zakresie metod i środków bezpieczeństwa. Powyższe cele, zgodnie z założeniami omawianej strategii, zamierza się realizować przez: system koordynacji przeciwdziałania i reagowania na zagrożenia i ataki na cyberprzestrzeń, powszechne wdrożenie wśród jednostek administracji rządowej oraz podmiotów niepublicznych mechanizmów służących zapobieganiu i wczesnemu wykrywaniu zagrożeń oraz właściwego postępowania w przypadku incydentów, a także edukację szerokich rzesz społeczeństwa w tym obszarze.

Bibliografia

Adamski A. (1998), *Karalność hackingu na podstawie przepisów kodeksu karnego z 1997*, „PS", nr 11–12.

Adamski A. (2000), *Prawo karne komputerowe*, Warszawa.

Adamski A. (2001), *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu konwencji Rady Europy*, Toruń.

Bączek P. (2005), *Zagrożenia informacyjne a bezpieczeństwo Państwa Polskiego*, Toruń.

Biała Księga Bezpieczeństwa Narodowego RP (2013), Biuro Bezpieczeństwa Narodowego, Warszawa.

Bógdał-Brzezińska A., Gawrycki M. F. (2003), *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa.

Ciborowski L. (1997), *Walka informacyjna*, Toruń.

Communication (2000) from the Commission of 11 April 2000 to the Council and the European Parliament „The organisation and management of the internet. International and European policy issues 1998–2000", COM (2000)202 final, http://europa.eu/legislation_summaries/information_society/internet/l24232_en.htm (28.2.2014).

Dawidziuk P., Łącki B., Stolarski M. P. (2009), *Sieć Internet – znaczenie dla nowoczesnego państwa oraz problemy bezpieczeństwa*, w: *Bezpieczeństwo teleinformatyczne państwa*, (red.) M. Madej, M. Terlikowski, Warszawa.

Decyzja Przewodniczącego Komitetu Rady Ministrów do spraw Cyfryzacji nr 1/2012 z 24 stycznia 2012 r. w przedmiocie powołania Zespołu zadaniowego do spraw ochrony portali rządowych (2012), Warszawa.

Europejski Internet? (2014), http://www.fronda.pl/a/europejski-internet-swietny-pomysl-angeli-merkel,34779.html (25.02.2014).

Fisher B. (2000), *Przestępstwa komputerowe i ochrona informacji. Aspekty prawne-kryminalistyczne*, Kraków.

Jordan T. (2011), *Hakerstwo*, Warszawa.

Kodeks karny. Część ogólna. Komentarz, t. I: *Komentarz do art. 1–116 k.k.* (2004), (red.) A. Zoll, Kraków.

Krasavin S. (2002), *What is Cyber-terrorism?*, http://www.crime-research.org/library/Cyber-terrorism.htm (3.01.2014).

Kulik M. (2011), *Przestępstwa piractwa komputerowego*, w: *System prawa karnego*, t. 9: *Przestępstwa przeciwko mieniu i gospodarcze*, (red.) R. Zawłocki, Warszawa.

Libicki M. (1995), *What is Information Warfare?*, Washington.

Madej M. (2009), *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego*, w: *Bezpieczeństwo teleinformatyczne państwa*, (red.) M. Madej, M. Terlikowski, Warszawa.

Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej (2013), Warszawa.

Rozporządzenie Prezesa Rady Ministrów z 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (2011), Warszawa.

Rządowy program ochrony cyberprzestrzeni RP na lata 2009–2011 – założenia (2009), Warszawa.

Sanz T. L. (1998), *Information – Age Warefare: A Workinh Bibligraphy*, „Military Review", Vol. LXXVIII, No. 2.

Sheehan M. (2000), *Statement before Senate Foreign Relations Committee*, Washington.

Skrzypczak J. (2013), *European Architecture of Data Communications Security as a Foundation in Information Society*, Berlin.

Siwicki M. (2013), *Cyberprzestępczość*, Warszawa.

Suchorzewska A. (2010), *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Warszawa.

Terlikowski M. (2009), *Bezpieczeństwo teleinformatyczne państwa a podmioty pozapaństwowe. Haking, haktywizmi cyberterroryzm*, w: *Bezpieczeństwo teleinformatyczne państwa*, (red.) M. Madej, M. Terlikowski, Warszawa.

Ustawa Kodeks karny z 6 czerwca 1997 r. (1997), Dz. U., nr 88, poz. 553 z późn. zm.

Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne z dnia 17 lutego 2005 r. (2005), Dz. U., nr 156, poz. 1301 z późn. zm.

Ustawa o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej z 21 marca 1991 r. (2003), Dz. U., nr 153, poz. 1502 ze zm.

Ustawa o ochronie danych osobowych z 29 sierpnia 1997 r. (2002), Dz. U., nr 101, poz. 926, z późn. zm.

Ustawa o ochronie granicy państwowej z 12 października 1990 r. (1990), Dz. U., nr 78, poz. 461 z późn. zm.

Ustawa o ochronie informacji niejawnych z dnia 5 sierpnia 2010 r. (2010), Dz. U., nr 182, poz. 1228 z późn. zm.

Ustawa o stanie klęski żywiołowej z 18 kwietnia 2002 r. (2002b), Dz. U., nr 62, poz. 558.

Ustawa o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej z 29 sierpnia 2002 r. (2002d), Dz. U., nr 156, poz. 1301.

Ustawa o stanie wyjątkowym z 21 czerwca 2002 r. (2002c), Dz. U., nr 113, poz. 985.

Ustawa o świadczeniu usług drogą elektroniczną z 18 lipca 2002 r. (2002a), Dz. U., nr 144, poz. 1204, z późn. zm.

Ustawa Prawo telekomunikacyjne z 16 lipca 2004 r. (2004), Dz. U., nr 171, poz. 1800, z późn. zm.

Wróbel W. (2013), *Przestępstwa przeciwko ochronie informacji*, w: *Kodeks karny, część szczególna*, tom III, (red.) A. Zoll, Warszawa.

Zarządzenie Ministra Obrony Narodowej z 20 października 2006 r. w sprawie nadania statutu Służbie Kontrwywiadu Wojskowego (2006), Warszawa.

Zarządzenie nr 73 Prezesa Rady Ministrów z 26 czerwca 2002 r. w sprawie nadania statutu Agencji Bezpieczeństwa Wewnętrznego (2002), Warszawa.

STRESZCZENIE

Celem niniejszego opracowania jest analiza założeń polityki ochrony cyberprzestrzeni RP zaprezentowanych w dokumencie zatytułowanym Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej, zaprezentowanym w 2013 r. przez *Ministerstwo Administracji i Cyfryzacji* i *Agencję Bezpieczeństwa Wewnętrznego*. Artykuł poddaje analizie postulaty i wytyczne tam zamieszczone, jak również konfrontuje te założenia z elementami systemu ochrony cyberprzestrzeni RP. Zgodzić należy się z twórcami tej strategii, iż zapewnienie stanu pełnego bezpieczeństwa teleinformatycznego, jest niemożliwe. Można mówić jedynie osiągnięciu pewnego, akceptowalnego jego poziomu. Wydaje się, że do osiągnięcia tego celu, powinna w znaczącym stopniu przyczynić się realizacja priorytetów polityki ochrony cyberprzestrzeni RP, a wśród nich w szczególności określenie kompetencji podmiotów odpowiedzialnych za bezpieczeństwo cyberprzestrzeni, stworzenie i realizacja spójnego dla wszystkich podmiotów administracji rządowej systemu zarządzania bezpieczeństwem cyberprzestrzeni oraz ustanowienie wytycznych w tym zakresie dla podmiotów niepublicznych, stworzenie trwałego systemu koordynacji i wymiany informacji pomiędzy podmiotami odpowiedzialnymi za bezpieczeństwo cyberprzestrzeni i użytkownikami cyberprzestrzeni, zwiększenie świadomości użytkowników cyberprzestrzeni w zakresie metod i środków bezpieczeństwa.

POLAND'S CYBER-SPACE PROTECTION POLICY

ABSTRACT

The article's objective was to analyse the premises of the policy concerning the Republic of Poland's cyber-space protection, presented in the document entitled *The policy of protecting the cyberspace of Republic of Poland*, published by the Ministry of Administration and Digitization of Poland and the Internal Security Agency in 2013. The current article examines the postulates and guidelines included therein, and also confronts them with selected elements of the system of Poland's cyber-space protection. The author is ready to agree with the creators of the strategy discussed that the complete management of the tele-information risk is impossible. It may only be feasible to attain a certain, acceptable level of such management. The implementation of the priorities of the discussed policy may, presumably, contribute considerably to this end. Particularly important in this context are the following: precise definition of competencies of entities responsible for cyber-space security, creation and implementation of uniform, for all entities of the government administration, a system of management of cyber-space risk, as well as formulation of related guidelines for non-public entities, and also creation of permanent system of coordination and exchange of information between entities responsible for cyber-space security and the cyber-space users themselves, and finally, making the latter fully realise the methods and measures of assuring cyber-space security.